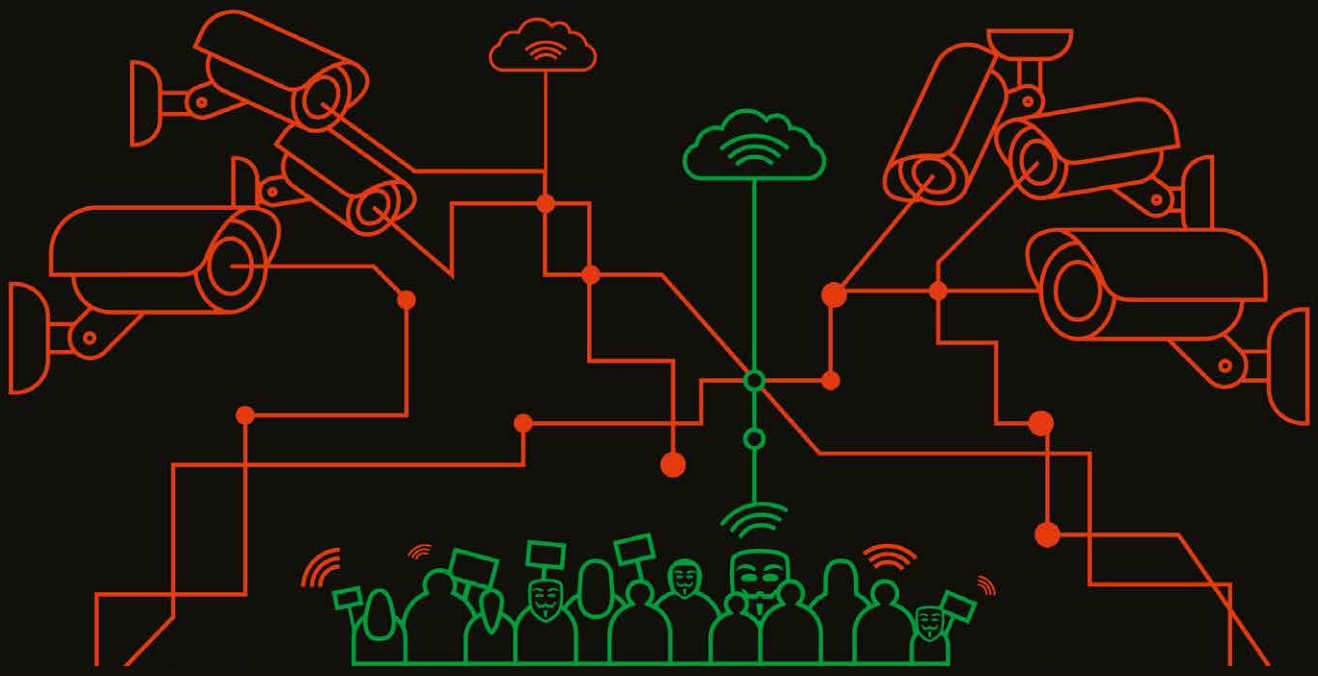

HackerWatch Roundup

Pro-Democracy Protests Amid State Surveillance and Hacktivist Competition

Filterwatch

July - December 2022

Executive Summary

The second edition of Hacker Watch report covers the latest developments in Iran's cyber orbit. Yet the report is overshadowed by the "Woman, Life, Freedom" movement, sparked by the tragic death of a young Kurdish woman in police custody in September 2022. These protests happened against a backdrop of expansive surveillance and geopolitical competition between Iran and Israel. As a result, the report focuses on two key themes:

First, it provides an overview of Iran's cyber capabilities that facilitate targeting of dissidents and attacking networks of Iran's adversaries.

In particular, the report focuses on Iran's surveillance apparatus developed in collaboration with private entities, based on new revelations from media reports and hacktivist personas.

Second, HackerWatch reviews Iran's cyber vulnerabilities as indicated by a series of ostensibly organic hacktivist attacks on the networks of state and its affiliated organizations. The resulting image suggests Iran's increased risk tolerance in targeting adversaries in the name of national security and, at the same time, deprioritizing resources for securing national networks, which undermines the collective sense of security for Iranian citizens.

Introduction

In September 2022, pro-democracy protests erupted in Iran following the death of 22-year old Mahsa Jina Amini in the custody of the so-called morality police, most likely as a result of police brutality. Protests that started with demanding accountability for Amini's death, gender equality, and respect for women's rights quickly turned into intersectional anti-regime rallies that mobilized ethnic, religious, gender equality, labor, and student activists alike. These nation-wide pro-democracy calls were unprecedented since the 2009 Green Movement and took the international community by surprise. Iran quickly moved to suppress the protests.

Not only did protesters face the risk of detention by security forces on the ground, but also they struggled with an expansive state surveillance apparatus that undermined their physical safety and integrity of communications on and off protest sites. Many people were arrested in their residence after their smartphones were tracked via telecom towers they had connected to during protests, others were identified through device registration numbers that the government has been collecting for the past years. During these protests, more details came to light about Iran's far-reaching surveillance capabilities, targeting political dissidents, ethnic and human rights activists, possible criminals, even ordinary citizens.

This expansive apparatus is developed in large part in collaboration with the private sector and numerous front companies that help Iran's security forces evade detection despite an extensive sanctions regime developed by the United States. This report explores the contribution of private entities to Iran's surveillance apparatus that continues to enable the government to suppress dissent on demand.

Iran has repeatedly cited national security reasons for expanding its cyber capabilities in the past two decades. Since the mid-2000s, Iran has grown its cyber capability to pursue a multi-pronged policy of curbing dissent at home, shaping regional geopolitics, and retaliating against adversaries – all at relatively low costs. Under this calculus, Iran has supported various hacking groups and used allegedly hacktivists personas to target political dissidents as well as Iran's arch adversaries, including Israel, Saudi Arabia, and the United States, with espionage, sabotage, or ransomware attacks. This report reviews multiple such groups with a wide range of targets, including a religious minority community, Israeli businesses, even the Albanian government.

Despite significant investments to posture as a cyber power, Iran remains extremely susceptible to cyber attacks. Ostensibly anonymous hacktivist groups presenting as dissidents have repeatedly targeted Iran's civilian networks with espionage and sabotage attacks. While attribution of these attacks is not certain, at least one incident from 2021 against gas pumps has been linked to Israel. These escalatory intelligence and sabotage operations in and through cyberspace correspond to the growing tension between the two countries and undermine Iranians' secure and reliable access to public digital infrastructure.

Recent protests in Iran gave fodder to this fire. Multiple purportedly hacktivist groups sprang in support of protesters, took down government websites, and leaked confidential documents, including the state's alleged strategy for undermining the protests. Unlike some previous attacks that indiscriminately impacted the public (e.g. shutting down the gas pumps), recent activities primarily focused on disrupting government activities and disclosing agents of suppression. They mirrored the chants of protesters on the street, creating a sense of trust and solidarity with many Iranian protesters. These revelations particularly shed light on the extent of collaboration between hardliner media and the military and intelligence apparatus in forming repressive policies. Unprecedented leaks also exposed the extra-legal mandate of various entities that facilitate an expansive surveillance system. This report presents a survey of some of these groups for a more detailed view of their activities.

However, speculations about the origin of these personas persist. A possible connection to state actors, like Israel, using hacktivism for covert operations can undermine digital safety of protesters in the long term. The more hacktivism is used as cover for damage

to domestic networks, the more Iran will be motivated to retaliate, even against dissidents. To deter from promoting hacked-and-leaked materials, Iran can utilize a simple post on social media to press bogus charges related to disruption of public order or inciting violence. Iran may also expedite hack-and-leak operations of its own as a tactic to intimidate opposition leaders and spread distrust among dissidents.

There are signs that Iran may be acknowledging the damage done by recent leaks, seeking better data protection for pro-regime entities and individuals. However, any lessons learned must apply indiscriminately to all domestic networks. Otherwise, Iran risks enabling further inequality in and through cyberspace by depriving the public from basic cybersecurity standards to protect their personal information. Iran's deprioritizing of cybersecurity for domestic networks will keep it vulnerable to blows from state and non-state threat actors – and civilian taxpayers will pay the price. Iran's lack of good governance in cybersecurity has consequences for public resources and the collective enjoyment of safety as a basic human right.

Iran's Cyber Capabilities

Domestic Attacks

July 2022 – The Bahai's Application

In July 2022, cybersecurity specialists of the Baha'i faith warned about the security of a new application called "The Baha'is" (اهل بها in Persian). The software first became publicly available through a Telegram channel that was created under the same name in February 2022. The channel catered to the Baha'i community and encouraged them to install the app. This was no ordinary application, however. "The Baha'is" was not available through official app stores like Google Play. It came in a large (50GB) APK file that could only be downloaded via the Baha'is Telegram channel.

Upon further investigation, Baha'i cybersecurity professionals discovered a backdoor in the application code that enabled access to users' data. The app was linked to two different Internet Protocol (IP) addresses. The first was linked to the app's menu (e.g. prayers, religious ceremonies). The second IP, however, extracted personal information from connected devices and saved it on an unknown server linked to a fictitious company in London. This IP has links to

the infrastructure used in other cyber operations from 2019 by Iranian hacking group MuddyWater.

MuddyWater is a cyber espionage group that, since at least 2017, has targeted a range of government and private organizations across different sectors, including telecommunications, local government, defense, and oil and natural gas organizations, in the Middle East, Asia, Africa, Europe, and North America. In January 2022, U.S. Cyber Command attributed MuddyWater to Iran's intelligence apparatus.

July and August 2022 – Labdookhtegan

On July 16, 2022, the anti-Iranian regime whistleblower persona LabDookhtegan (aka Read My Lips) published the names of at least 15 individuals that allegedly worked for two front companies of the IRGC. LabDookhtegan developed this list based on revelations from investigative journalist Bob Diachenko.

In February 2022, Diachenko published a redacted, extensive database of personal information of Iranian citizens, linking social media accounts to phone numbers, voter and car registration, phone geolocation, and more. The database was hosted on a now-defunct website *secnerd[.]ir* that LabDookhtegan linked to "Najee Technology," an IRGC front company headed by Mansur Ahmadi.[1] LabDookhtegan also identified a second front company of the IRGC's intelligence and cyber services, Afkar System headed by Ahmad Khatibi.

LabDookhtegan published documents indicating a link between these two companies and known IRGC-linked cyber actors like Cobalt Mirage, Charming Kitten,[2] and TunnelVision. In the past years, these groups have been detected in ransomware and other types of malicious cyber activities against targets worldwide.

October 2022 – The SIAM System

This was not the only time that Iranian authorities were called out for mass surveillance of Iranians in recent months. In October 2022, online news site *The Intercept* published a detailed account of a previously unreported instrument of Iranian state censorship,

1 A fringe OSINT website DaeshHunter claimed a link between SECNERD and Mansur Ahmadi and his company, Najee Technology, in May 2022, two months before LabDookhtegan.

2 Charming Kitten has a long history of conducting phishing attacks against political activists, analysts, and other regional experts. In a latest attempt, Charming Kitten was detected posing as well-known authors or think-tank leaders to bait area experts for phishing their credentials.

the SIAM system. It is a web program for remotely manipulating cellular connections made available to the Iranian Communications Regulatory Authority (CRA).

According to internal documents from Ariantel, an Iran-based Mobile Virtual Network Operator (MVNO), that The Intercept reportedly obtained from a hacker, SIAM enables its operators to alter, disrupt, and monitor how customers use their phones. This is broadly done by matching the phone numbers that have connected to specified cell towers with their corresponding IMEI number, a unique string of numbers assigned to every mobile phone in the world.

This type of tracking makes common privacy-preserving tactics like SIM card swapping ineffective in Iran since IMEI numbers persist even with a new SIM. Moreover, the SIAM system can also significantly slow data connections from 3G or 4G connection to 2G, break the encryption of phone calls by forcing 2G bandwidth which entails many vulnerabilities, track the movements of individuals or large groups, and produce detailed metadata of individual communications, including voice, SMS, and data usage.

In short, SIAM is a legal intercept system that could help the government suppress dissent and protests on demand. However, this system would constitute a significant departure from standardized lawful intercept standards developed by 3GPP working groups and ETSI standards committees. These standards define processes and interfaces for the exchange of legal warrants, activation of communication interception, and delivering the communication content to the legal authority.

October 2022 – Domestic Kitten

The SIAM system is not the only tool of the Islamic Republic for spying on its citizens. In October, researchers at cybersecurity firm ESET detected Domestic Kitten, a state-linked threat actor that has been active since at least 2016, to be targeting Iranians with spyware.

Domestic Kitten is known to conduct mobile surveillance operations targeting Iranians and anti-government groups in the Middle East. Cybersecurity firm Check Point first disclosed an extensive Domestic Kitten campaign in 2018 that targeted Iranian citizens of Kurdish and Turkish descent and, in some cases, ISIS supporters. The surveillance operation has been ongoing since 2016, using Android malware that compromised mobile data such as contact lists, phone call records, text messages, and more.

Since June 2021, Domestic Kitten has distributed a malware known as FurBall masquerading as an Android translation app "sarayemaghale.apk". This malicious application is delivered via a fake website mimicking a legitimate Iran-based site (downloadmaghaleh.com) for downloading articles and books translated from English to Persian (see Figure 1 for a comparison between the two sites).

The fake website distributed an Android app for download. However, instead of directing users to Google Play as the download button claims, this app downloads directly from the attacker's server. In October 2022, ESET researchers identified a new version of this app that requested fewer intrusive permissions (access to contacts only) compared to the original Furball malware that could access SMS messages, device location, call logs, and clipboard data. The change is most likely designed to evade detection and possibly to facilitate further social engineering through spearphishing of the victim's contacts via text messages.

Figure 1. Significant resemblance between the fake website used by Domestic Kitten (left) and the legitimate website (right). Source: ESET

International Attacks

July 2022 – Attacks against Israeli Targets

Last summer, multiple Israeli targets from public and private sectors reported incidents that contained traces of Iranian cyber activities. In July, a self-proclaimed Iraqi hacking group Al-Tahera claimed responsibility for attacks against several commercial and public sector websites, including Tel Aviv's municipality and Israeli's mass

transit system. Then in August, Iranian threat actor Mercury (Muddy Water) was detected in the exploitation of Log4j 2 vulnerabilities against Israeli organizations.

Mercury (Muddy Water)

In August 2022, Microsoft Threat Intelligence Center (MSTIC) detected Iran-based threat actor MERCURY (aka Muddy Water) leveraging exploitation of Log4j 2[3] vulnerabilities in several tools offered and managed by SysAid, a global IT management company. Muddy Water used these vulnerabilities in SysAid tools to get initial access to the networks of Israeli targets.

After gaining access, Muddy Water establishes persistence, dumps credentials, and moves laterally within the targeted organization using both custom and known hacking tools, as well as built-in operating system tools (Figure 2).

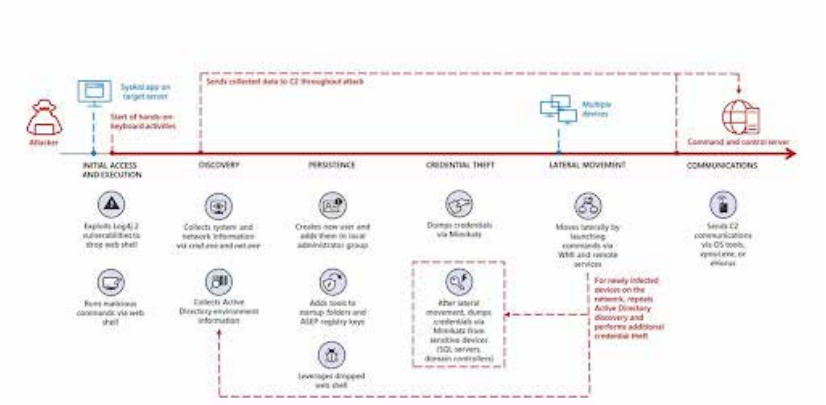

Figure 2. MERCURY (Muddy Water) attack chain. Source: Microsoft

Al-Tahera

NTA Mass Transit Company

On July 4, Telegram channel Al-Tahera (Arabic for Pure, spelled ALtahrea by the group itself), a little-known self-proclaimed Iraqi hacking group published news and screenshots of an alleged “attack”

3 Log4j is a coding framework that is developed by Apache and used in various software applications and services. In December 2021, Apache warned about vulnerabilities in Log4j that malicious threat actors were exploiting for intrusions to various systems. Around the same time, Iranian threat actor Charming Kitten was detected actively using basic open-source tools for Log4j exploitation, suggesting that the group had rushed to leverage the vulnerability. Log4 j 2.0 is a new iteration of the framework with new features and several bug fixes.

on the "Tel Aviv metro" and claimed responsibility for it. The group's messaging is close to that of the Iraqi *muqawama* militia (i.e. Popular Mobilization Forces (PMF)), a regional ally of the IRGC's Quds Force Unit. Muqawama is Arabic for resistance.

Shortly after the announcement, Sabereen News, media affiliate of PMF along with pro-muqawama and pro-Iran Twitter accounts promoted the news. They claimed that the attack had affected Tel Aviv metro's operating systems, control monitors, and servers. In a few hours, Iran's official English outlet, Press TV, and semi-official Fars News Agency covered the incident as well.

The news, however, turned out to be a misinformation campaign at best – or worse, complete disinformation. There is no metro system in Tel Aviv. Instead, a light rail system is under construction by state-owned company NTA and is the subject of a political debate in Israel. Al-Tahera claims seem to refer to a limited distributed denial-of-service (DDoS) attack on the NTA website as well as its associated IP addresses.[4]

Tel Aviv Municipality

In July 2022, al-Tahera continued with additional DDoS attacks against Israeli targets. On July 11, the group claimed responsibility for defacing Tel Aviv's municipality website with a message that read "Do not work suspended order if General Qassem Soleimani [sic]". The vengeful message was an apparent reference to Israel's involvement in the U.S. drone strike on Qassem Soleimani and his Iraqi trenchmate, Abu Mahdi Al-Muhandis.

PMF Telegram channel Sabereen News once again promoted the incident, claiming a cyberattack originating from Iraq targeted "computer networks of Tel Aviv's municipality." Iranian hardline media, such as IRGC-affiliate Tasnim News, and pro-Iran Lebanese outlet Al-Mayadeen promoted the announcement as well. On July 14, the group targeted the Jerusalem municipality website with a similar attack that did not receive nearly as much media traction.

Public and Commercial Websites

On July 17, al-Tahera claimed responsibility for hacking Israel's ministry of health in response to the bombing of the Gaza Strip

4 A DDoS attack overwhelms a website with near-simultaneous traffic and queries to send it offline. It does not enable data theft.

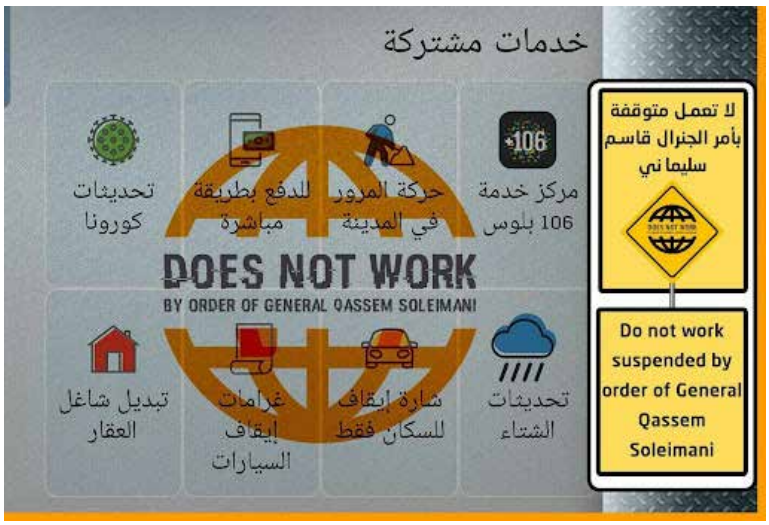

Figure 3. Al-Tahera hacking group defaced the website of Tel Aviv municipality on July 11, 2022. Source: Al-Tahera Telegram channel.

the day before and a list of other ills. Israel hit the Gaza Strip twice during the weekend of July 16 in response to rockets fired at Israeli communities from the Palestinian territory. Israel's Ministry of Health stated that access to its website was disrupted only for users connecting from abroad but remained functional for local users.

On July 26, Al-Tahera announced more defacements of 19 Israeli commercial websites where they placed an image of Qassem Soleimani. Iran's Fars News and Tasnim News promoted the incident, touting the capability of the Iraqi hacking group.

The alleged Iraqi origin of Al-Tahera and promotional campaigns from PMF's media outlet Sabereen News fit its purported motivation to take revenge for the killing of Soleimani and Al-Muhandis. However, Iraq has little history of pursuing cyber attacks which raises the possibility of alternative origins of Al-Tahera. This includes training or material support from Iran, as PMF's main ally, or an outright Iranian group posing as Iraqi muqawama cyber fighters.

While the exact origin and relationship between al-Tahera and Iran's cyber threat actors remains unclear, the extensive media coverage of the incident suggests links between these groups. In the past, Iran has used fictitious hacking groups like Yemen Cyber Army as a front for obfuscating its cyber campaigns' true origin. Al-Tahera may well be the latest front for Iran's cyber activities against regional rivals.

July 2022 – Attacks against Government of Albania

On July 15, 2022, Iran-sponsored actors conducted a destructive cyberattack against the Albanian government, disrupting

government websites and public services. In addition, a separate yet simultaneous Iran-sponsored actor leaked sensitive information that had been exfiltrated months earlier (as early as May 2021). Various websites and social media outlets were used to leak this information. The attacks forced Albania to temporarily shut down government systems, including online public services and government websites.

The attacks occurred one week ahead of the annual Mujahedeen-e-Khalq-(MEK)-sponsored Free Iran World Summit. The summit, which was scheduled for July 23-24 in the city of Manëz of the Durres county, Albania, was canceled following warnings of possible terrorist threats to the Summit on July 21. The summit convenes annually to bring together MEK members and other MEK-aligned individuals opposed to the Islamic Republic.

The MEK (also known as MKO or PMOI), is an Iranian opposition organization that seeks to overthrow the regime in Tehran. It was formerly designated as a terrorist organization by the U.S. Department of State until 2012. The group has been based in camp Ashraf 3 in Manëz, Albania (about 30 kilometers west of Tirana).

On July 22, "HomeLand Justice," a self-proclaimed hacking group allegedly run by Albanian citizens, claimed credit for the disruptive attack against Albanian government websites. The group posted a video of the ransomware on its .ru domain (homelandjustice.ru) and Telegram channel.[5] It also published alleged Albanian government documents and residence permits and other personal information of MEK members.

The group's logo is an eagle preying on the symbol of the hacking group "Predatory Sparrow" (Gonjesh-e-Darandeh in Persian) inside the Star of David (Figure 4). This signals the attack on Albania as retaliation for Predatory Sparrow's operations against Iran, in at least one of which Israel's involvement has been confirmed. Predatory Sparrow has claimed responsibility for several high-profile cyberattacks against state-linked entities in Iran since July 2021. This included attacks on Iran's gas pumps in October 2021, steel conglomerate in July 2022, and disruption of television programming of the Islamic Republic of Iran Broadcasting (IRIB) with images saluting MEK leaders in January 2022. Iranian officials have repeatedly blamed these attacks on the MEK and Israel.

5 The original website and Telegram channel are no longer available. Internet Archive has stored some of the website pages and there is a backup Telegram channel that was created on August 31, 2022.

Iranian cyber actors and pro-Iran information operations have frequently targeted the MEK with malware, antagonistic messaging, even forged materials. The latest attacks, however, are a geographic expansion of Iranian disruptive cyber operations, conducted against a NATO member state. They may indicate an increase in Iran's risk tolerance when it deems appropriate to secure its national and geopolitical interests.

Figure 4. Ransomware image and Homeland Justice banner

In September 2022, Microsoft assessed with high confidence that at least four actors were involved in the attacks, each performing distinct tasks. These actors deployed the ransomware and wiper malware on target systems and exfiltrated data and probed the victim's infrastructure upon gaining access to those networks. Microsoft also assessed with moderate confidence that the actors involved in gaining initial access and exfiltrating data in the attack are linked to EUROPIUM (aka APT 34 or OilRig), which has been publicly linked to Iran's Ministry of Intelligence and Security (MOIS).

In response, Albania severed diplomatic relations with Iran on September 7, 2022 and became the first known country to sever diplomatic ties over a cyberattack. It ordered Iranian diplomats and embassy staff to leave within 24 hours. The United States supported the move and responded by designating Iran's (MOIS) and its Minister of Intelligence for engaging in cyber-enabled activities against the United States and its NATO ally Albania. Iran, for its part, has categorically denied any involvement in the attacks and strongly opposed the closure of its embassy. If anything, immediately following the severance of diplomatic ties, Albania's prime minister Edi Rama disclosed that the same actors had attacked government systems again on September 9. The brazen move underscores Iran's increased tolerance of risk and its willingness to persist with malicious behavior.

Iran's Cyber Vulnerabilities

Despite Iran's efforts to posture as a cyber power, it continues to suffer from blows to its networks, infrastructure, and secrets. These cyberattacks underscore serious failures in securing computer network systems even at the highest levels of government. One of the consistent threats Iran has been dealing with since at least 2021 is alleged hacktivist groups conducting hack-and-leak operations – and occasional sabotage attacks. This trend soared as the "Woman, Life, Freedom" protests erupted in September 2022 following the death of Mahsa Jina Amini in the morality police custody.

As the protests continued and state restrictions on Internet access intensified, multiple hacking groups used platforms like Signal, Telegram, even the dark web to aid anti-government protesters in Iran. These activities came in different forms, including data leaks from prominent institutions like IRGC affiliates, disclosing personal data of local officials and state operators involved in the suppression of protesters, and dissemination of circumvention tools for continued access to the Internet. This, however, was not merely an increase in the number of attacks against Iran's networks, but also an expansion of hacktivist personas.

R2O

Previously, hacktivist personas like Revolt to Overthrow (R2O) defaced multiple government websites with anti-regime and pro-MEK messages and leaked confidential documents. It also targeted the SMS and CCTV systems of Tehran municipality. In July, R2O breached six websites and 44 servers associated with the Organization of Islamic Culture and Communications (one of the state entities in charge of production and dissemination of Islamic propaganda) and allegedly accessed over 12,000 documents. In October, R2O reacted to the suppression of protesters and their sham trials by attacking servers of Iran's judiciary. It published purported personal information of over 63,000 judiciary staffers. Similar to its previous attacks, R2O also defaced the website of "Imam Khomeini and the Islamic Revolution's Research Center" with pro-MEK images and messaging.

Anonymous

Hacktivist collective Anonymous also made a comeback to the post-

protests hacking scene.[6] At the onset of protests, Anonymous, known for its activities during Occupy Wall Street and the Arab Spring, pledged its support for the people of Iran. On September 20, a person wearing a Guy Fawkes mask appeared in a video announcing a campaign called #OpIran, and vowed to shut down the government of Iran.

Since the YouTube video first appeared, Anonymous has allegedly hacked more than 1,000 CCTV cameras across Iran and launched distributed denial of service (DDoS) attacks against websites of multiple state bodies, including the Central Bank of Iran; official websites of the executive branch, including president.ir; the official portal of Supreme Leader Ali Khamenei;[7] and the website for the Telecommunications Company of Iran (TCI), a state-owned telecom entity, to name only a few of Anonymous targets. Anonymous also leaked the purported bank information of government officials and phone numbers of members of parliament — all in the name of #OpIran and Mahsa Amini.

Among Anonymous's activities in the past months, two stand out. On October 1, 2022 Iranians started receiving mass SMS invitations to anti-regime rallies. Anonymous claimed it had hacked Najva, a marketing telecommunications service for commercial text messages and push notifications. Najva's various clients include a wide range of companies, from hardliner news outlets like Fars News to online clothing retails (e.g. Bani Mode). As Anonymous took over Najva's servers, anti-regime text messages were sent on behalf of these clients to a large pool of mobile owners in Iran. Najva confirmed the breach and shut down its servers for a few hours.

On October 13, Anonymous warned about a piece of malware that was detected on Android devices of the protesters who were detained and released by state security forces. Anonymous alleged that malware L3MON installed a remote control program on the victim's phone for access to all personal information, including pictures, phone

6 This was not the first time that Anonymous targeted the Iranian government. In June 2009, amid the Green Movement protests that emerged in response to the disputed re-election of Mahmoud Ahmadinejad, Anonymous launched an earlier version of Operation Iran (OpIran) — a DDoS campaign targeting government websites and government-affiliated organizations. In February 2011, as Iranians took to the streets to support the Arab Spring, Iran sought to suppress the protests through mass arrests and renewed censorship. In response, OpIran was resurrected, launching DDoS attacks against government websites, including the websites of the Supreme Leader and the president. Later that year, in the run-up to the anniversary of the 2009 Iranian presidential election, Anonymous leaked more than 10,000 emails from the Ministry of Foreign Affairs that contained visa requests and passport images of non-Iranians. However, these incidents were not widely noted by Iranians at the time. Read more on DFRLab.

7 Army of Thieves, a self-proclaimed Israeli hacking group, also claimed a "heavy, two-day" DDoS attack against Khamenei's website on the same day that Anonymous publicized its own attack (September 22, 2022).

numbers, and text messages. Anonymous recommended to protesters (a) to not take their personal phone to protests, and (b) to assume that their smartphones were infiltrated with malware as soon as they were arrested and their devices confiscated. In this case, Anonymous recommended, the best way forward would be to reset devices to

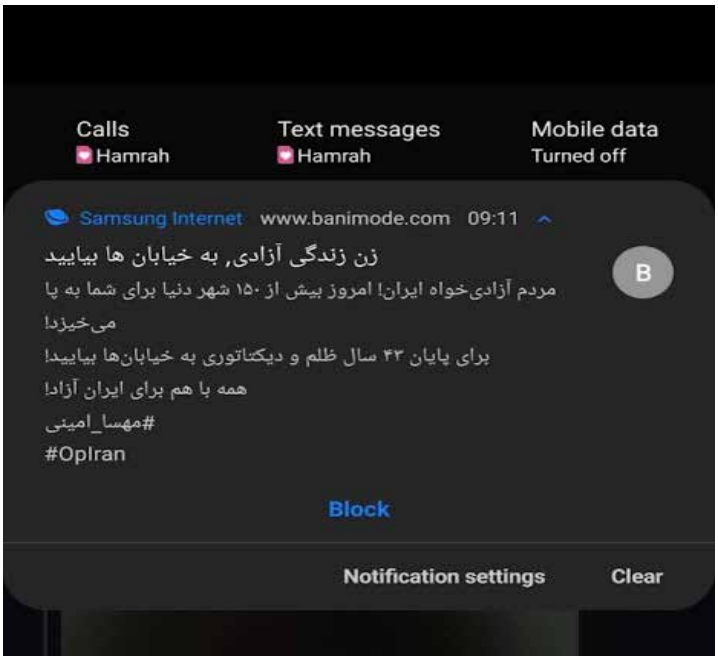

Figure 5. Sample SMS invite to an anti-regime rally sent via Najva on behalf of Bani Mode, an online clothing retail shop.

factory settings and notify contacts of potentially being exposed to state hackers.

On November 3, Anonymous released a tranche of hacked documents from the Committee on Identification of Criminal Content. The entity is a contentious bureau within the office of Prosecutor General of Iran's judiciary that determines which online content should be censored. These emails, however, revealed the committee's extensive mandate that enables further surveillance of Iranians.

For example, in one leaked email from 2021, the committee demanded the administrators of Aparat, the domestic version of YouTube, to reveal the identity of an account holder on the platform without citing a specific reason for such a query. Within days, Aparat complied and shared the email and multiple IP addresses associated with the account.

In a separate email from 2020, a year before Ebrahim Raisi was elected president, revealed that in his capacity as the head of judiciary, Raisi was a staunch supporter of filtering all circumvention tools and tightening the grip on any social media and messaging

apps that remained unblocked (e.g. Instagram and WhatsApp). The revelation is at odds with Raeesi's claims during his presidential campaign, endorsing platforms like Instagram that were critical for the economy and self-employment.

Black Reward

Between July and December 2022, multiple other groups also made a debut appearance – a trend that only expedited following the protests. Among these groups was hacktivist persona Black Reward. On September 25, in reaction to the suppression of protesters, Black Reward purportedly defaced and wiped servers of Iran's Housing Foundation and multiple affiliated domains for their alleged association with the IRGC and contribution to corruption schemes. On October 19, BlackReward leaked internal emails of Press TV, the international arm of the state broadcaster. The emails shed light on Press TV's operations and inner workings, from unpaid invoices of up to $18,000 to high-ranking officials voicing their discontent with Russian outlet RT Arabic's coverage of Iran.[8]

In the days that followed, BlackReward released 50 GB worth of data from Iran's Atomic Energy Development Agency; released documents from the Islamic Culture and Communications Organization (the same entity that R2O also breached in July); hacked and released data from Iran's National Oil and Gas Company and tens of its private affiliates as well as the IRGC's Khatam-al-Anbiya Construction Headquarters (an engineering firm controlled by the IRGC).
In a matter of weeks, Black Reward single-handedly released more documents than any other hacktivist personas since the protests began. It was not just the sheer number of documents but also the nature of revelations that put Black Reward on the spotlight.

On November 25, BlackReward defaced the homepage of semi-official Fars News Agency (a key media affiliate of the IRGC) and replaced it with a blurred image of a women protester waving her headscarf, a move emblematic of the Woman, Life, Freedom movement. Four days later, on November 29, BlackReward released an alleged news bulletin that Fars News had prepared for high-ranking IRGC officials about the latest protests.

The bulletin was a controversial document, presumably pulled from Fars servers during the hack a few days earlier. It showed how the

8 This was seemingly in reference to RT's coverage of Iranian wrestler Navid Afkari's execution in 2020.

regime perceived the protests and tweaked facts in its own favor. For example, the bulletin underscored the dissatisfaction of Supreme Leader Khamenei with president Raeesi and the police commanders for their inefficient handling of the protests. At the same time, the Supreme Leader allegedly asked for measured moves (instead of outright arrest) to undermine the credibility of influential figures like Sunni cleric, Molavi Abdul Hamid from Sistan and Baluchestan and a staunch supporter of protesters in 2022.

The Fars bulletin was emblematic of an open secret that Iranians had suspected for years: that hardliner media were critical players in Iran's intelligence apparatus, in particular the IRGC. They inform highest ranking commanders of the latest sociopolitical developments and provide analysis that in turn shape Iran's response to sensitive events such as protests.

By the end of December, Black Reward released multiple tranches of Fars-related materials, including internal documents, astronomical paystubs of high-ranking managers, politically sensitive interviews that were recorded but never published, and an audio recording of a meeting of hardliner officials, where they discussed the protests and possible ways forward. A controversial revelation from the meeting was that the Qatari government had allegedly shared information about Iranian passport holders attending the 2022 World Cup (hosted by Qatar) and pledged to help the Iranian government to suppress anti-regime protests at the tournament.

Tapandegan

On October 13, 2022, a new hacktivist persona Tapandegan infiltrated the online portal of Iran's Al-Zahra University, an all-female higher education institution historically known for its obsessive religious rules around hijab and admission requirements.

Tapandegan defaced the university's portal to display a national call to rally along with safety instructions for protesters (Figure 6). On November 29, Tapandegan leaked key information about at least two IRGC contractors that facilitate the Quds Force's presence in Syria to support Bashar Al-Assad's regime. These documents claim that commercial entities such as "Milad" and "Surin Special Group (SSG)" perform as the Quds Force's intermediary on the ground, offering security and construction services in different parts of Syria.

Figure 6. Tapandegan defaced the online portal of Al-Zahra University in Tehran on October 13, 2022.

Barandazan

On November 2, another little-known persona Barandazan (Persian for overthrowers) also targeted Al-Zahra University and leaked internal documents. These revelations mostly portray behind the operations scene of the university since the protests began.

One document, in particular, disclosed a request for bonuses for the campus security personnel to boost morale while they continued to suppress student protesters. As college students prepared for more protests and nation-wide strikes on December 7 (the national day of students in higher education), Barandazan hacked over a hundred domains belonging to 16 Iranian universities, including Al-Zahra.

The group promised to publish 8 GB of documents and data (excluding students' personal information) in the following days. However, the group's Telegram channel has not posted since then.[9]

Conclusion

In the second half of 2022, Iran continued its malicious activities against targets that it deems a threat to national security. The distribution of targets followed a typical pattern: domestic and diaspora dissidents, on one hand, and foreign targets that Iran has

9 Barandazan also defaced the website of the State Accounts Court (دیوان محاسبات کشور) on November 22, allegedly in retaliation for the suppression of protesters in Kurdistan and Sistan and Balochistan provinces.

historically and ideologically conflicted with on the other hand. Israel is a prime example. Iran-linked hacking personas continued to target Israeli commercial targets with disruptive but less sophisticated attacks, such as DDoS. One important development, however, was the audacity of Iranian threat actors to extend their operations into the NATO alliance by launching multi-stage, more disruptive ransomware and wiper malware attacks against the government of Albania. The motivation behind these attacks had domestic roots, linked with the Albanian government's hosting of the MEK. However, they may well be a prelude to how Iran's increased risk tolerance will alter its future cyber activities to shape geopolitical competition.

The report also observes expansive surveillance operations of the Islamic Republic against its own citizens. While Iran justifies surveillance programs like SIAM under national security, their far-reaching execution goes well beyond the alleged intended use. Under the guise of rule of law, such programs also violate the principles of proportionality and necessity as they often indiscriminately target a wide range of targets, including criminals, political dissidents, ethnic and human rights activists. Iran's abysmal record of human rights violations coupled with its malicious cyber capabilities only reinforce concerns about the role of its digital surveillance and censorship apparatus in undermining Iranians' rights.

Despite Iran's persistent efforts to posture as a cyber power, it remains extremely vulnerable to blows to its networks, infrastructure, and secrets. Allegedly hacktivist cyber attacks have intensified since the beginning of Woman, Life, Freedom protests last September. These cyberattacks underscore serious failures in securing computer network systems even at the highest levels of government. The situation poses a strategic dilemma to Iran. It needs to balance available resources between securing domestic networks and its malicious cyber operations. So far, Iran has repeatedly prioritized the latter over protecting state networks that the taxpayers' money sustains. It remains to be seen whether continued blows from foreign and domestic hacktivist personas can change Iran's calculus in favor of sustainable digital governance. We will continue to monitor related developments in future editions of Hacker Watch reports.